GIRARD SHARP LLP
Adam E. Polk (State Bar No. 273000)
Patrick T. Johnson (State Bar No. 329580)
601 California Street, Suite 1400
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
Email: apolk@girardsharp.com
Email: pjohnson@girardsharp.com

SAUDER SCHELKOPF LLC
Joseph G. Sauder (*Pro Hac Vice* forthcoming)
Joseph B. Kenney (*Pro Hac Vice* forthcoming)
Juliette T. Mogenson (*Pro Hac Vice* forthcoming)
1109 Lancaster Avenue
Berwyn, PA 19312
Telephone: (888) 711-9975
Facsimile: (610) 421-1326
Email: jgs@sstriallawyers.com
Email: jbk@sstriallawyers.com
Email: jtm@sstriallawyers.com

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

SACRAMENTO DIVISION

KRISTEN WARREN, CHRISTOPHER NEAL, AND C.N., individually and on behalf of all others similarly situated,

Plaintiffs,

v.

POWERSCHOOL HOLDINGS, INC. AND POWERSCHOOL GROUP LLC,

Defendants.

Case No:

CLASS ACTION COMPLAINT FOR:

1. **NEGLIGENCE**
2. **NEGLIGENCE PER SE**
3. **BREACH OF IMPLIED CONTRACT**

DEMAND FOR JURY TRIAL

Plaintiffs Kristen Warren, Christopher Neal, and C.N. ("Plaintiffs"), individually and on behalf of the proposed class defined below, bring this action against Defendant PowerSchool Holdings, Inc. and Defendant PowerSchool Group LLC ("PowerSchool" or "Defendants") and alleges as follows:

I. SUMMARY OF THE ACTION

1. PowerSchool is the largest provider of cloud-based education software in the United States. It is used by more than 18,000 customers, primarily K-12 educators, to support more than 50 million students— more than 75% of K-12 students in North America. As part of its business, PowerSchool maintains in its computer systems the personally identifying information ("PII" or "Private Information") and/or protected health information ("PHI") of 60 million people, including teachers, students, and their guardians.

2. Despite holding the highly sensitive personal information of millions of people—many of whom are minors—PowerSchool neglected to adequately secure it. Unbeknownst to its customers or the end users PowerSchool stored PII and PHI in unencrypted formats on an Internet-accessible environment, vulnerable to exploitation.

3. At some point between December 19 and December 28, 2024, hackers breached the company's vulnerable systems and exfiltrated the valuable PII and PHI stored within (the "Data Breach" or "Breach." PowerSchool learned of the Data Breach on December 28, 2024, and began to investigate. Beginning on January 8, 2025, PowerSchool began notifying customers that their data was accessed and they were impacted.

4. Now, Plaintiffs and other members of the proposed class must deal with the fallout. The attack exposed over 60 million individuals' PII and PHI in total. For impacted individuals, PII and PHI stolen in the Data Breach include Social Security numbers, dates of birth, addresses, phone numbers, emails, photo identification, tax information numbers, health histories, and other medical information. Plaintiffs' information continues to reside on or remain accessible through PowerSchool's systems.

5. Plaintiffs by this action seek compensatory and statutory damages as well as injunctive relief to remediate PowerSchool's deficient cybersecurity and provide credit

monitoring, identity theft insurance, and credit repair services (or the money needed to secure those services) to protect her and the other breach victims from identity theft and fraud.

II. PARTIES

6. Plaintiff C.N. is a minor under the age of 18. At all relevant times, he has been domiciled in the state of Ohio. Plaintiff C.N. attends school in the West Clermont School District.

7. Plaintiff Kristen Warren is the mother and legal guardian of Plaintiff C.N. At all relevant times, she has been domiciled in the state of Ohio.

8. Plaintiff Christopher Neal is the father and legal guardian of Plaintiff C.N. At all relevant times, he has been domiciled in the state of Ohio.

9. Defendant PowerSchool Holdings, Inc., is a Delaware corporation with its principal place of business at 150 Parkshore Dr., Folsom, California 95630.

10. Defendant PowerSchool Group LLC is a Delaware Limited Liability Company with its principal place of business at 150 Parkshore Dr., Folsom, California 95630.

11. Defendant PowerSchool Holdings, Inc. and PowerSchool Group LLC are collectively referred to as PowerSchool or Defendants.

12. At all relevant times, each Defendant was a principal, agent, alter ego, joint venturer, partner, or affiliate of each other, and in doing the acts alleged herein, was acting within the course and scope of that principal, agent, alter ego, joint venture, partnership, or affiliate relationship. Each Defendant had actual knowledge of the wrongful act of each other; ratified, approved, joined in, acquiesced, or authorized the wrongful acts of each other; and retained the benefits of those wrongful acts.

III. JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendants' states of citizenship.

14. This Court has personal jurisdiction over Defendants because they are headquartered in and have their principal place of business in this district. Defendants conduct substantial business and have minimum contacts with the State of California.

15. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendants are headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL BACKGROUND

A. Background on PowerSchool

16. PowerSchool holds itself out "[a]s a leading provider of cloud-based software in North America. Its product supports vast numbers of teachers, students, and their parents. Seventy-five percent of American school children, over 35 million, use PowerSchool. Over 16,000 customers rely on PowerSchool, including 90 of the largest 100 districts by student enrollment.

17. In 2024, Bain Capital acquired PowerSchool for $5.6 billion.

18. The data PowerSchool collects far exceeds traditional education records of school-age children, including thousands of person-specific data fields.

19. PowerSchool does not fully disclose what data it collects from school-age children or their parents.

20. PowerSchool refuses to provide children and parents access to their data or the information it generates using that data.

21. On information and belief, PowerSchool collects and maintains the PHI and PII of customers, including but not limited to:

a. name, residential address, phone number, and email address
b. date of birth
c. demographic information
d. Social Security number
e. tax identification number
f. financial information

g. medication information

h. disability information

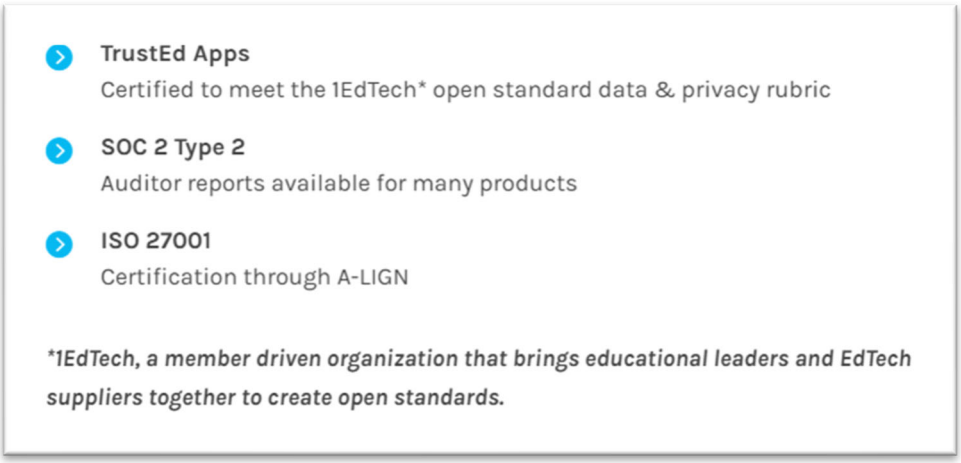
i. health insurance information

j. photo identification

k. employment information

B. PowerSchool's Data Security Representations

22. PowerSchool has multiple webpages dedicated to its privacy and security capabilities. It represents that it uses "industry standards" to "improve data integrity and security."[1] It claims that all products are "[c]ertified to meet the 1EdTech open standard data & privacy rubric," and have received "ISO 27001" certification through "A-LIGN."



23. In its privacy policy, PowerSchool boasts that it "places great importance and value on the proper handling of personal data that flows within our product as we provide services to our customers."[2] To this end, PowerSchool claims that it has the "relevant security and privacy policies to drive expectations from the workforce":

> We seek to protect our customers' personal data from unauthorized access, use, modification, disclosure, loss, or theft by leveraging various reasonable security measures and methods to secure our customers' personal data throughout its processing lifecycle with PowerSchool

[1] https://www.powerschool.com/interoperability-overview/ (last visited January 31, 2025).
[2] https://www.powerschool.com/privacy/ (last visited January 31, 2025).

> applications. Our overall aim is to ensure the confidentiality, integrity, and availability of our customers' personal data by leveraging technical, organizational, and where appropriate, physical security methods. Security protection at PowerSchool is a cross-functional activity that intersects our workforce duties, and we have relevant security and privacy policies to drive expectations from the workforce.[3]

24. Under the "Frequently Asked Questions," PowerSchool represents that it protects data by using "state-of-the-art, and appropriate physical, technical, and administrative security measures to protect the personal data that we process."[4]

25. PowerSchool's Global Privacy Statement, last updated October 1, 2024, makes the following representations about PowerSchool's data security measures:

> Whether PowerSchool is a collector or processor or your data, PowerSchool is committed to protecting your personal information. PowerSchool uses commercially reasonable physical, administrative, and technical safeguards to preserve the confidentiality, integrity, and availability of your personal information. Our systems are regularly certified by third parties against industry security standards from AIPCA and ISO. As customers provide PowerSchool with Customer Data to process, PowerSchool makes commercially reasonable efforts to ensure the security of our systems. Please note that this is not a guarantee that such information may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, administrative, and technical safeguards.
> …
> PowerSchool employs a variety of physical, administrative, and technological safeguards designed to protect your data against loss, misuse, and unauthorized access or disclosure. We strive to continuously maintain reasonable physical, administrative, and technical security measures. Our security measures consider the type and sensitivity of the data being collected, used, and stored, and the current state of technology and threats to data. PowerSchool independently verifies its security management system to the internationally recognized standard for security management and holds ISO 27001 and SOC2 certifications. PowerSchool also endeavors to align its privacy and security operations to best practices and relevant international regulations.[5]

---

[3] *Id.*
[4] *Id.*
[5] *Id.*

C. The Data Breach

26. On December 22, 2024, hackers successfully breached PowerSchool's computer systems and exfiltrated customer PII and PHI. According to PowerSchool's breach notice, the hack occurred through the "PowerSchool customer support portal," which allowed "further access to the company's school information system, PowerSchool SIS." This is the information system schools use to manage student records, grades, attendance, and enrollment. PowerSchool learned of the hack six days later, on December 28, 2024, after the hackers contacted them to issue a ransom.

27. PowerSchool investigated the Data Breach and identified the compromised products and customers. It confirmed that the breach affected "families and educators." On January 8, 2025, it publicly announced the Data Breach and began notifying customers.

28. By failing to protect Plaintiffs' and Class members' PII and PHI, PowerSchool breached its duties and violated its privacy promises to its members and beneficiaries.

D. PowerSchool Failed to Maintain Adequate Cybersecurity Measures to Prevent the Data Breach.

29. PowerSchool did not reasonably and adequately protect the PII and PHI of its customers or their students, families, and educators.

30. According to PowerSchool's notification letter to affected clients, the hackers gained access "using a compromised credential."

31. PowerSchool was unable to prevent hackers from gaining access to its systems, detect that hackers had gained access to its systems and sensitive patient information, or determine that a breach had occurred until the hackers contacted them with a ransom demand.

32. PowerSchool failed to implement and maintain reasonable security measures to prevent and detect the Data Breach, such as auditing and monitoring its data retention, encryption, deletion, and vendor practices.

E. PII and PHI have concrete financial value

33. PHI and PII are inherently valuable, and they are becoming increasingly frequent targets of hackers. The PII and PHI taken from PowerSchool's systems are particularly sensitive.

34. Medical records and personally identifiable information are valuable to cybercriminals and routinely are sold and traded on the dark web. There is a robust black market in which criminals openly post stolen PHI and PII on multiple underground internet websites, commonly referred to as the dark web.

35. Identity theft results in a significant, negative financial impact on victims as well as severe distress.

36. PHI and PII are valuable commodities to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes, including identity theft and medical and financial fraud. There is accordingly a market for Plaintiffs' and Class members' PHI and PII.

37. PHI is particularly sensitive. Healthcare data can sell for as much as $363 per record, according to the Infosec Institute.[6] PHI is especially valuable because criminals can use it to target victims with fraud and scams that take advantage of the victim's medical conditions or settlements. PHI can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or to gain access to prescriptions for illegal use or resale.

38. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, misdiagnosis or mistreatment can ensue. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," said Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[7]

39. Similarly, Social Security numbers are valuable to criminals. This information can be, and has been, sold and traded on the dark web. The loss of a Social Security number is

[6] https://resources.infosecinstitute.com/topics/healthcare-information-security/hackers-selling-healthcare-data-in-the-black-market/ (last accessed January 31, 2025).

[7] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/ (last accessed January 31, 2025).

particularly troubling because it cannot be easily changed and can be misused in a range of nefarious activities, such as filing fraudulent tax returns to steal tax refund payments, opening new accounts to take out loans, and other forms of identity theft.

40. The detrimental consequences of PowerSchool's failure to keep its customers', students', families', and educators' PHI and PII secure are long lasting and severe. Once PHI and PII are stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for months or years.

41. Children are particularly vulnerable targets in a data breach. Identity theft can result in malicious actors running up debts before the child even turns 18. The child might be unaware of these debts until years later when they enter into the credit market to apply for loans or financial aid.

42. Criminals often trade stolen PHI and PII on the dark web for years following a breach. Cybercriminals also can post stolen PHI and PII on the internet, thereby making the information publicly available without the knowledge or consent of the victim.

43. PowerSchool knew the importance of safeguarding the PHI and PII entrusted to it and the foreseeable adverse effects if its data security systems were breached. Those effects include the significant costs that would be imposed on affected students, their parents, and educators as a result of a breach. PowerSchool failed to implement reasonable and adequate cybersecurity measures, leading to the Data Breach.

F. PowerSchool Owed Duties to Safeguard Individuals' PII and PHI

44. Beyond the obligations arising from PowerSchool's own representations keeping Plaintiffs' and Class Members' data secure, Defendants owed Plaintiffs and Class members a duty to safeguard their PII and PHI.

45. As described further below, Defendants owed a duty to safeguard PII and PHI under several statutes, including the Federal Trade Commission Act ("FTC Act") and the Children's Online Privacy Protection Act ("COPPA"), to ensure that all information they maintained was secure. These statutes were enacted to protect Plaintiffs and the Class members from the type of conduct in which Defendants engaged.

46. Defendants owed a duty to safeguard PII and PHI because they were on notice that they were handling highly valuable data and knew there was a risk it would be targeted by cybercriminals. Moreover, Defendants knew of the extensive, foreseeable harm that would ensue for the victims of a data breach, and therefore owed a duty to safeguard that information.

47. Given the sensitive nature of the PII and PHI routinely contained in Defendants' systems, Defendants knew that hackers and cybercriminals would be able to commit identity theft, financial fraud, phishing, socially-engineered attacks, healthcare fraud, and other identity-related fraud upon exfiltrating that data from Defendants' system. Defendants also knew that individuals whose PII and PHI were maintained Defendants' system would reasonably spend time and effort to mitigate their damages and prevent identity theft and fraud, if that PII and PHI were taken.

48. Defendants also owed a duty to safeguard Plaintiffs' and Class members' data based upon the promises that they made to their clients and customers to securely store data. Defendants voluntarily undertook efforts to keep that data secure in their business operations and thus owe a continuing obligation to Plaintiffs and Class members to keep their PII and PHI secure.

49. The duty to protect Plaintiffs' PII and PHI is non-delegable. PowerSchool's business model is premised upon voluntarily assuming this duty, by soliciting customers to rely on its professed ability to store sensitive data securely. PowerSchool's duty is for the benefit of the individuals whose PII and PHI its products store and manage.

50. Defendants also owed a duty to comply with industry standards in safeguarding PII and PHI, which they did not do.

51. Because of the value of PII and PHI to hackers and identity thieves, companies in the business of storing, maintaining, or securing PII and PHI such as Defendants, have been identified as being particularly vulnerable to cyberattacks. Cybersecurity firms have promulgated a series of best practices that at a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management

systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

52. Federal and state government bodies have likewise established security standards and issued recommendations to reduce the risk of data breaches and the resulting harm to consumers and financial institutions. The FTC has issued numerous guides for businesses highlighting the importance of robust and effective data and cyber security practices. According to the FTC, the imperative of data and cyber security should be factored into all business decision-making.

53. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data and cyber security principles and practices for business. The guidelines note businesses should protect the personal customer and consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines further recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

54. The FTC also recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

55. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ appropriate measures to protect against unauthorized access to confidential consumer data as an unfair

practice that violates Section 5 of the FTC Act, 15 U.S.C. § 45. Orders in these actions further clarify the measures businesses must take to meet their data and cyber security obligations.

56. Further, pursuant to COPPA, 15 U.S.C. § 312.10, Defendants had a "mandate[d]" duty to only "retain children's personal information 'for only as long as is reasonably necessary to fulfill the purpose for which the information was collected[,]'" and thereafter had a duty to "delete [children's personal information] using reasonable measures to ensure it's been securely destroyed" even absent a parent's request for the deletion of a child's personal information.

G. Plaintiffs' PHI and PII were Compromised in the Data Breach

57. Plaintiffs Kristen Warren and Christoper Neal are a married couple and parents of C.N. All are citizens and residents of Ohio. C.N. attends school in the West Clermont School District.

58. As part of C.N.'s schooling, Plaintiffs Kristen Warren and Christopher Neal provided PowerSchool their child's sensitive PII and PHI and provided sensitive PII of themselves.

59. On January 9, 2025, Plaintiffs received an email from their school stating that PowerSchool had informed them that the Plaintiffs' school had been affected by the Data Breach. The school's notice conveyed PowerSchool's representations that had "contained" the incident and that the hackers had "deleted" the data.

60. Plaintiffs greatly value their privacy, and the privacy of their minor child. Because of PowerSchool's failure to protect the sensitive information entrusted to it, Plaintiffs are less safe now than they were before the breach.

61. Plaintiffs have suffered actual injury in the form of damages to and diminution in the value of their PII and the PII of their child— a form of intangible property that they entrusted to PowerSchool in exchange for education support and administration services.

62. The exposure of Plaintiffs' private and confidential information, including health information, in the Data Breach has caused Plaintiffs to suffer stress and anxiety related to their personal information being compromised.

63. Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII and PHI, and the PII and PHI of their child, especially with their child's Social Security number indefinitely in the hands of criminals.

64. Plaintiffs have become victims of hacking and blackmail attempts by criminal actors that obtained their PII and PHI as a result of the Data Breach.

65. Specifically, Plaintiff Christopher Neal experienced a fraud attempt using information that was subject to the Data Breach. A hacker posed as an Ohio governmental representative and threatened to garnish Plaintiff Neal's wages. Plaintiff Neal has expended time and resources to report and resolve this unauthorized attempt.

66. Additionally, Plaintiff Christopher Neal has become a target of a blackmail attempt. A criminal actor obtained his PII and PHI from the Data Breach and has threatened Plaintiff Christopher Neal and his family if he does not pay the criminal actor. Plaintiffs have expended time and resources to report and resolve this blackmail attempt.

67. Because of the Data Breach, Plaintiffs are at a substantial present risk both with respect to their personal safety and increased risk of identity theft and fraud, and will continue to face an increased risk for years to come.

68. Plaintiffs and Class members must immediately devote time, energy, and money to: (1) closely monitor their medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them. Plaintiffs and Class members have taken or will be forced to take these measures in order to mitigate their potential damages as a result of the Data Breach.

69. Plaintiffs have a continuing interest in ensuring that their PII and PHI, which remain in PowerSchool's possession, are protected and safeguarded from future breaches.

V. CLASS ACTION ALLEGATIONS

70. Plaintiffs bring this class action on behalf of themselves and all others similarly situated pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and where applicable, 23(c)(4), on behalf of the following Class:

> **Class:** All natural persons in the United States whose PII and/or PHI was compromised as a result of the Data Breach.

71. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

72. Plaintiffs reserve the right to modify the Class definition, including based on discovery and further investigation.

73. Numerosity. The Class is so large as to make joinder impracticable. There are millions of Class members. Disposition of their claims in a single action will provide substantial benefits to all parties and to the Court. Class members are readily ascertainable from information and records in the possession, custody, or control of Defendants or its customers.

74. Typicality. Plaintiffs' claims are typical of the claims of the Class in that the sensitive personal information of the representative Plaintiffs, like that of all Class members, was compromised and stolen in the Data Breach.

75. Adequacy of Representation. Plaintiffs are members of the Class and will fairly and adequately represent and protect its interests. Plaintiffs' counsel are competent and experienced in prosecuting class actions, including relating to data breaches. Plaintiffs have no interest contrary to or in conflict with the interests of Class members.

76. Predominant Common Issues of Law and Fact. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual Class members. Among the questions of law and fact common to the Class are:

- Whether Defendants engaged in the conduct alleged;
- Whether Defendants had a duty to implement reasonable cyber security measures to protect Plaintiffs' and Class members' sensitive, personal information;
- Whether Defendants breached its duty by failing to take reasonable precautions to protect Plaintiffs' and Class members' sensitive, personal information;
- Whether Defendants acted unfairly or otherwise wrongfully in violation of state statutory law;
- Whether Plaintiffs and Class members are entitled to recover damages; and
- Whether Plaintiffs and Class members are entitled to equitable relief, including injunctive relief, restitution, and/or disgorgement.

77. Superiority. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Absent a class action, most Class members would likely find the cost of litigating their claims prohibitively high and would have no effective remedy. Given the relatively small size of the individual Class members' claims, few, if any, Class members would seek redress for Defendants' violations individually. Class treatment will conserve the resources of the courts and promote consistency and efficiency of adjudication.

Class certification is also appropriate under Rules 23(b)(1), (b)(2), and/or (c)(4) because:

- The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications establishing incompatible standards of conduct for Defendants.
- The prosecution of separate actions by individual Class members would create a risk of adjudications that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests.
- Defendants have acted or refused to act on grounds generally applicable to the Class, making injunctive and corresponding declarative relief appropriate with respect to the Class as a whole; and

- The claims of Class members are comprised of common issues whose resolution in a class trial would materially advance this litigation.

FIRST CAUSE OF ACTION
Negligence

78. Plaintiffs incorporate and reallege the foregoing allegations of fact.

79. Defendants collected and stored Plaintiffs' and Class members' personal information, including addresses, Social Security numbers, dates of birth, health insurance information, and personal health information including disabilities, immunization records, and medications.

80. Defendants owed Plaintiffs and Class members a duty of reasonable care to preserve and protect the confidentiality of their personal information that it collected. This duty included, among other obligations, maintaining and testing its security systems and networks, and the systems and networks of its vendors, as well as taking other reasonable security measures to safeguard and adequately secure the personal information of Plaintiffs and the Class from unauthorized access and use.

81. Defendants' duties also arise by operation of statute. Pursuant to the FTC Act, 15 U.S.C. § 45, PowerSchool had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PHI and PII.

82. Plaintiffs and Class members were the foreseeable victims of Defendants' inadequate and ineffectual cybersecurity systems and protocols. The natural and probable consequence of Defendants' failing to adequately secure its information networks was Plaintiffs' and Class members' personal information being hacked.

83. Defendants knew or should have known that Plaintiffs' and Class members' personal information was an attractive target for cyber thieves, particularly in light of data breaches experienced by other entities around the United States. Moreover, the harm to Plaintiffs and Class members from exposure of their highly confidential personal information was reasonably foreseeable to Defendants.

84. Defendants had the ability to sufficiently guard against data breaches by monitoring and testing their systems and implementing adequate measures to protect their systems, such as using attack surface software.

85. Defendants breached their duty to exercise reasonable care in protecting Plaintiffs' and Class members' personal information by failing to implement and maintain adequate security measures to safeguard Plaintiffs' and Class members' personal information, failing to monitor its systems to identify suspicious activity, and allowing unauthorized access to, and exfiltration of, Plaintiffs' and Class members' confidential personal information.

86. There is a close connection between Defendants' failure to employ reasonable security protections for its members and beneficiaries' personal information and the injuries suffered by Plaintiffs and Class members. When individuals' sensitive personal information is stolen, they face a heightened risk of identity theft and may need to: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries and charges; (5) place and renew credit fraud alerts on a quarterly basis; (6) contest fraudulent charges and other forms of identity theft; (7) repair damage to credit and financial accounts; and (8) take other steps to protect themselves and attempt to avoid or recover from identity theft and fraud.

87. Defendants were in a special relationship with Plaintiffs and Class members with respect to the hacked information because the end and aim of Defendants' data security measures was to benefit Plaintiffs and Class members by ensuring that their personal information would remain protected and secure. Only Defendants were in a position to ensure that its systems were sufficiently secure to protect Plaintiffs' and Class members' personal and medical information. The harm to Plaintiffs and Class members from their exposure was foreseeable to Defendants.

88. The policy of preventing future harm disfavors the application of the economic loss rule, particularly given the sensitivity of the private information entrusted to Defendants. A high degree of opprobrium attaches to Defendants' failure to secure Plaintiffs' and Class members' personal and extremely confidential facts. Defendants had an independent duty in tort to protect this information and thereby avoid reasonably foreseeable harm to Plaintiffs and Class members.

89. As a result of Defendants' negligence, Plaintiffs and Class members have suffered actual and/or nominal damages that have included or may, in the future, include, without limitation: (1) loss of the opportunity to control how their personal information is used; (2) diminution in the value and use of their personal information entrusted to Defendants with the understanding that Defendants would safeguard it against theft and not allow it to be accessed and misused by third parties; (3) the compromise and theft of their personal information; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and unauthorized use of financial accounts; (5) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports, and assets; (6) unauthorized use of compromised personal information to open new financial and other accounts; (7) continued risk to their personal information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the personal information in their possession; and (8) future costs in the form of time, effort, and money Plaintiffs and Class members will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

SECOND CAUSE OF ACTION

Negligence *per se*

90. Plaintiffs incorporate and reallege the foregoing allegations of fact.

91. Under Section 5 of the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information.

92. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI they obtained and stored and the foreseeable consequences of a data breach involving PII of their consumers.

93. Plaintiffs and Class members are consumers within the Class of persons Section 45 of the FTC Act was intended to protect.

94. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

95. The harm that has occurred as a result of Defendants' conduct is the type of harm that the FTC Act and Part 2 were intended to guard against.

96. Further, pursuant to COPPA, 15 U.S.C. § 312.10, Defendants had a "mandate[d]" duty to only "retain children's personal information 'for only as long as is reasonably necessary to fulfill the purpose for which the information was collected[,]'" and thereafter had a duty to "delete [children's personal information] using reasonable measures to ensure it's been securely destroyed" even absent a parent's request for the deletion of a child's personal information.

97. Defendants violated COPPA § 312.10 by failing to use reasonable measures to protect PII and PHI and not complying with industry standards.

98. Plaintiffs and Class members are consumers within the Class of persons COPPA was intended to protect.

99. Defendants' violation of COPPA constitutes negligence *per se*.

100. The harm that has occurred as a result of Defendants' conduct is the type of harm that COPPA was intended to guard against.

101. As a direct and proximate result of Defendants' negligence, Plaintiffs have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION

Breach of Implied Contract

102. Plaintiffs incorporate and reallege the foregoing allegations of fact.

103. Defendants contracted with Plaintiffs' and the Class members' schools and/or school districts for the provision of education software. These contracts include, without limitation, Defendants' privacy notices in which they promised to protect nonpublic personal information given to Defendants, or which Defendants gathered on their own, from disclosure. These privacy notices include Defendants' Global Privacy Statement.

104. Plaintiffs and Class members are the intended beneficiaries of those contracts, including the provisions incorporating Defendants' privacy policies and otherwise pertaining to the confidentiality of personal information maintained by Defendants.

105. Plaintiffs and Class members performed substantially all that was required of them under their contracts with Defendants, or they were excused from doing so.

106. Defendants explicitly acknowledged their obligation to protect Plaintiffs' and Class members' confidential information in these contracts. In their Global Privacy Statement, Defendants state that PowerSchool "uses commercially reasonable physical, administrative, and technical safeguards to preserve the confidentiality, integrity, and availability of your personal information."

107. A meeting of the minds occurred, as Plaintiffs and other Class members agreed, among other things, to provide their PII and PHI to Defendants for which Defendants derived a monetary benefit, in exchange for Defendants' agreement to protect the confidentiality of that information.

108. No Plaintiff would have entered into these contracts with Defendants without understanding that Plaintiffs' and other Class members' PII and PHI would be safeguarded and protected. In short, data security was a material term of the parties' contracts.

109. Defendants breached these promises by failing to comply with reasonable industry practices, and by allowing unauthorized users to gain access to Plaintiffs' and Class members' PII and PHI through the Data Breach.

110. As a direct and proximate result of Defendants' breach of contract, Plaintiffs and Class members did not receive the full benefit of the bargain, and instead received education services that were less valuable than promised in their contracts. Plaintiffs and Class members,

therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Defendants' deficient performance.

111. As a result of Defendants' breach of contract, Plaintiffs and Class members have suffered actual damages resulting from the exposure of their personal information, remain imminent risk of suffering additional damages in the future, and/or are otherwise entitled to nominal damages.

112. Plaintiffs and Class members have consequently been injured by Defendants' breach of contract and are entitled to damages and/or restitution in an amount to be proven at trial. Plaintiffs seek nominal damages in the alternative.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for an order:

A. Certifying this case as a class action, appointing Plaintiffs as a Class representative, and appointing Plaintiffs' counsel to represent the Class;

B. Entering judgment for Plaintiffs and the Class;

C. Awarding Plaintiffs and Class members monetary relief, including nominal and statutory damages;

D. Ordering appropriate injunctive or other equitable relief;

E. Awarding pre- and post-judgment interest as prescribed by law;

F. Awarding reasonable attorneys' fees and costs as permitted by law; and

G. Granting such further and other relief as may be just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: January 31, 2025

Respectfully submitted,

By: /s/ *Patrick T. Johnson*

Adam E. Polk (State Bar No. 273000)
Patrick T. Johnson (State Bar No. 329580)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, California 94108

Telephone: (415) 981-4800
Facsimile: (415) 981-4846
Email: apolk@girardsharp.com
Email: pjohnson@girardsharp.com

Joseph G. Sauder (*Pro Hac Vice* forthcoming)
Joseph B. Kenney (*Pro Hac Vice* forthcoming)
Juliette T. Mogenson (*Pro Hac Vice* forthcoming)
SAUDER SCHELKOPF LLC
1109 Lancaster Avenue
Berwyn, PA 19312
Telephone: (888) 711-9975
Facsimile: (610) 421-1326
Email: jgs@sstriallawyers.com
Email: jbk@sstriallawyers.com
Email: jtm@sstriallawyers.com

Counsel for Plaintiffs